UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,013	01/18/2002	David Kammer	035451-0170 (3708.Palm)	2103

26371 7590 08/31/2006

FOLEY & LARDNER LLP
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/053,013	KAMMER ET AL.	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25 and 27-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25 and 27-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 23 June 2006.

2. The examiner would like to point out that this action is made **FINAL** (MPEP 706.07a).

3. Claims 1-25, 27-53 are pending in the application.

4. Claims 1-25, 27-53 have been rejected.

Response to Arguments

5. Regarding the rejections of claim 1-25 and 27-51, the applicant primarily argues that independently or in combination the references Stewart et al or Bade et al or Zillikens et al does not teach or suggest:

(a) selecting a single level of security from a group of more than two security levels..wherein the group of more than two security levels is defined by a user of the network user node.

(b) a storage device for storing a table of security modifications...., the security modifications being defined by a user of the network user node.

However, the examiner respectfully disagrees with the applicant's above argument(s).

Stewart et al does teach:

(a) selecting a single level of security from a group of more than two security levels (Fig 5, element : identification information comprising plurality of access levels associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location)....wherein the group of more than two security levels is defined by a user of the network user node (Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device; Col 3, lines 15-28; Col 8, lines 44-50; Col 10, line 65 to Col 11, lines 3; the access information may be

provided by the PCD of the user; plurality of the systems such as AP, MIB, or PCD with memory to support/ manage the access features; using PCD instead of access point/ MIB) .

(b) a storage device for storing a table of security modifications (Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device; Col 8, lines 44-50; Col 14, lines 39-55; Claim 11; maintaining; MIB; PCD)...., the security modifications being defined by a user of the network user node(Col 3, lines 15-28; Col 8, lines 44-50; Col 10, line 65 to Col 11, lines 3; the access information may be provided by the PCD of the user; plurality of the systems such as AP, MIB, or PCD with memory to support/ manage the access features; using PCD instead of access point/ MIB) .

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 2-5, 7-9, 11-13, 15-16, 18, 19-21, 23-24, 27-28, 30, 31-36, 38, 39-41, 43-44, and 46-48 are rejected under 35 USC 102 (b) as being anticipated by Stewart et al (Patent No: 6970927 B1).

Regarding claim 1, Stewart et al teaches a method of adjusting security for a network user node in a communication with network based upon the location of the node, comprising:

determining the location of a network user node (Col 8, lines 26-42; Col 20, lines 1-10; determining geographic location of the portable computing device) ;

selecting a single level of security from a group of more than two security levels based on the determined location (Fig 5, element : identification information comprising plurality of access levels

associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location), the group of more than two security levels being stored in the memory of the network use node (Col 6, lines 10-30; Col 19, lines 47-67; supporting multiple access levels; Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device); and

modifying the security protection for the network user node based upon the selected level of security (Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device; Col 7, lines 5-25; Col 8, lines 26-40; Col 10, lines 24-40; Col 20, lines 1-35; access level is based on geographic location; providing network access to the portable computing device based on the access level);

wherein the group of more than two security levels is defined by a user of the network user node (Col 3, lines 15-28; Col 8, lines 44-50; Col 10, line 65 to Col 11, lines 3; the access information may be provided by the PCD of the user; plurality of the systems such as AP, MIB, or PCD with memory to support/ manage the access features; using PCD instead of access point/ MIB).

Regarding claim 18, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches a computer system for modifying security settings for a network user node based on the location of the node (Col 8, lines 26-42; Col 20, lines 1-10; determining geographic location of the portable computing device) comprising:

an input device having a communicative coupling with a system for determining the location of a network user node (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location);

a storage device for storing a table of security modifications to be performed based on a plurality of locations for the network user node, the security modifications including more than two levels (Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device; Col 14, lines 39-55; Claim 11; maintaining; MIB/ PCD memory);

a processor coupled to a storage device for processing information, storing on a storage device, and generating a security modification instruction (Col 5, lines 50-67; PCD with wireless Ethernet card; Col 21, lines 60-67; Col 22, lines 1-10; determine the access level for the portable computing device by accessing the memory medium); and

a communication device capable of transmitting a data signal to the network user node containing instructions to modify the security protection for the node (Col 7, lines 5-25; Col 8, lines 26-40; Col 10, lines 24-40; Col 20, lines 1-35; access level is based on geographic location; providing network access to the portable computing device based on the access level).

Regarding claim 30, it is rejected applying as above rejecting claim 18, furthermore, Stewart et al teaches a method of adjusting security for a network user node having a processor, a memory coupled to the processor, a wireless transceiver, and a location determining device in communication with a network based upon the physical location of the node (Col 21, lines 10-67; Col 22 ,lines 1-15), comprising:

receiving physical location information using a network user node (Fig 4, element 206: AP transmits geographic location to network; Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location); and

using a network user node to modify security protection for data to a single level from a group of more than two levels, based upon the physical location information (Fig 5, element : identification information comprising plurality of access levels associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location).

Regarding claim 38, it is rejected applying as above rejecting claim 30, furthermore, Stewart et al teaches a system implemented on a network user node for modifying security settings based on the physical location of the node comprising:

a system for determining the physical location of the network user node coupled to the network user node (Fig 4, element 206: AP transmits geographic location to network; Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location);

a processor for processing information, storing information on a storage device (Col 5, lines 50-67; PCD with wireless Ethernet card; Col 21, lines 60-67; Col 22, lines 1-10; determine the access level for the portable computing device by accessing the memory medium), and

accessing a table of security modification instructions, the table including more than two unique security modifications (Col 6, lines 10-30; Col 19, lines 47-67; supporting multiple access levels; Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level is stored in a memory comprised in a portable computing device); and

a storage device coupled to the network user node for storing a table of security modifications; (Col 20, lines 25-59; first, second access levels; the identification information, wherein the access level

is stored in a memory comprised in a portable computing device; Col 14, lines 39-55; Claim 11; maintaining; MIB/ PCD memory);

wherein the network user node performs security modifications based on the physical location of the network user node (Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location).

Regarding claim 2, it is rejected applying as above rejecting claim1, furthermore, Stewart et al teaches network user node is a mobile device having a display (Col 5, lines 59-67; Col 6, lines 1-10; portable computing device/ PCD, PDA).

Regarding claim 3, it is rejected applying as above rejecting claim1, furthermore, Stewart et al teaches the network user node's location is determined using a location sensing system (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location).

Regarding claim 4, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches the location sensing system is a global positioning satellite (GPS) system (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location).

Regarding claim 5, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches location sensing system uses signal bouncing and triangulation to determine network user node location (Col 2, lines 8-16; wireless network comprising Access Points, AP; Col 8, lines 26-42; providing geographic locations information of PCD through AP).

Regarding claim 7, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches network user node is in direct communication with the location sensing system (Col 8, lines 26-42).

Regarding claim 8, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches sending a data signal includes transmitting the data signal using a wireless local area network (WLAN) protocol (Col 10, lines 1-25, 55-67;wireless LAN).

Regarding claim 9, it is rejected applying as above rejecting claim 8, furthermore, Stewart et al teaches WLAN protocol includes the IEEE 802.11 protocol (Col 10, lines 1-25, 55-67; IEEE 802.11; wireless LAN).

Regarding claim 11, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches the selecting step is carried out by reference to a table of desired security modifications based upon the location of network user node (Fig 5, element: table of identification information and associated access information; Col 7, lines 30-67; table comprising identification and access control information).

Regarding claim 12 it is rejected applying as above rejecting claim 11 furthermore, Stewart et al teaches security levels are provided by the user of the network user node for a variety of locations (Col 19, lines 60-67; Col 20, lines 1-20; Col 21, lines 10-40; Col 23, lines 45-50; plurality of access points; plurality of portable devices; wireless network of portable devices).

Regarding claim 13, it is rejected applying as above rejecting claim 11 furthermore, Stewart et al teaches the security level is based on the type of location determined for the network user node (Fig 5, element : identification information comprising plurality of access levels associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location).

Regarding claim 15, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches the step of modifying the security protection for the network user node includes a complete denial of access to information using the network user node (Fig 4, element 226: disallowing access; Col 20, lines 5-35; if the access level is the second access level, the data is not provided).

Regarding claim 16, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches denial to a subset of the information accessible using the node (Col 7, lines 5-30; Col 20, lines 5-35; providing appropriate level of access; providing access to one or more resources depending on permission level).

Regarding claims 19-21, 23-24, 27-28, they recite the limitations of claims 1, 2-5,7-9, 11-13, and 18, therefore, they are rejected applying as above rejecting claims 1, 2-5,7-9, 11-13 and 18.

Regarding claims 31-36, they recite the limitations of claims 1, 2-5,7-9, 11-13, and 30, therefore, they are rejected applying as above rejecting claims 1, 2-5,7-9, 11-13 and 30.

Regarding claims 39-41, 43-44, and 46-48, they recite the limitations of claims 1, 2-5,7-9, 11-13, and 38, therefore, they are rejected applying as above rejecting claims 1, 2-5,7-9, 11-13 and 38.

Regarding claim 50-53, they recite the limitations of claim 1,18,30, 38, therefore, they are rejected applying as above rejecting claim 1,18,30 and 38, furthermore, Stewart et al teaches network user node is a portable handheld device (Col 5, lines 59-67; Col 6, lines 1-10; portable computing device/ PCD, PDA).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6, 10, 14, 22, 25, 37, 42, and 45 are rejected under 35 USC 103 (a) as being unpatentable over Stewart et al (Patent No: 6970927 B1) in view of Bade et al (Pub No: 2002/0138632 A1).

Regarding claim 6, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al discloses location sensing system to determine network user node location (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location).

Stewart et al fails to disclose the use of signal bouncing and triangulation for that purpose.

However, Bade et al discloses the use of signal bouncing and triangulation to determine network user node location (Page 2, Par[0023]; GPS system, pinpointing location using 3D triangulation).

Bade et al and Stewart et al are analogous art because they are from the same field of endeavor of using geographic/ physical location information for providing access security/ authentication in a wireless network system. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teaching of Bade et al with Stewart et al to use signal bouncing and triangulation as a part of location sensing system to determine network user node location. Motivation for doing so would have been simply that techniques such as signal bouncing and triangulation are widely used in GPS system, or that such triangulation techniques can be used in positional access system to pinpoint the geographic location using GPS system (Bade et al , Page 2, Par [0023]).

Regarding claim 10, it is rejected applying as above rejecting claims 6 and 8, furthermore, Bade et al discloses WLAN protocol includes Bluetooth wireless network protocol (Page 2, Par

[0023]; 3D triangulation; GPS system; Bade et al 's teachings of "3D triangulation" and "GPS system" implies use of Bluetooth or any suitable/ popular wireless network protocol for that purpose).

Regarding claim 14, it is rejected applying as above rejecting claims 1 and 6, furthermore, Stewart et al discloses the step of modifying the security protection for the network user node includes restricting access to information (Col 7, lines 5-25; Col 8, lines 26-40; Col 10, lines 24-40; Col 20, lines 1-35; access level is based on geographic location; providing network access to the portable computing device based on the access level; Col 14, lines 39-55; Claim 11; maintaining).

Stewart et al fails to disclose use of a password for that purpose.

However, Bade et al discloses restricting access to information unless a password is properly entered (Page 2, Par [0012], Col 1, lines 1-8; Page 3, Par [0030]; determining whether access should be granted or denied, or requires a special password).

Regarding claims 22, 25, they recite the limitations of claims 6, 10, 14, and 18, therefore, they are rejected applying as above rejecting claims 6, 10, 14, and 18.

Regarding claims 37, 42, and 45, they recite the limitations of claims 6, 10, 14, 30, and 38, therefore, they are rejected applying as above rejecting claims 6, 10, 14, 30, and 38.

8. Claims 17, 29, and 49 are rejected under 35 USC 103 (a) as being unpatentable over Stewart et al (Patent No: 6970927 B1) in view of Zillikens et al (Patent No: 6813503 B1).

Regarding claim 17, it is rejected applying as above rejecting claims 1, furthermore, Stewart et al fails to disclose the step of modifying the security protection for the network user node includes modifying data encryption parameters to change the strength of encryption on data transmitted by the network user node.

However, Zillikens et al discloses modifying the security protection for the network user node includes modifying data encryption parameters to change the strength of encryption on data transmitted by the network user node (Col 19, lines 53-62; Col 21, lines 1-18;encrypted wireless communication; encrypted format, in order to provide a level of security when transmitting wireless information).

Zillikens et al and Stewart et al are analogous art because they are from the same field of endeavor of providing secure wireless communication utilizing location information . At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teaching of Zillikens et al with Stewart et al to modify the security protection for the network user node includes modifying data encryption parameters to change the strength of encryption on data transmitted by the network user node. Motivation for doing so would have been simply to provide a high level of security in wireless data transferring (Zillikens et al, Col 7, lines 30-50).

Regarding claims 29 and 49, they recite the limitations of claims 17, 18, and 38, therefore, they are rejected applying as above rejecting claims 17,18, and 38.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

NASSER MOAZZAMI
PRIMARY EXAMINER